Remarks

Claims 1-38 are pending in the application. Claims 1-38 were rejected. Claims 1 and 26 are the independent claims. Reconsideration of the application in view of the following remarks is respectfully requested.

The examiner rejected claims 1-38 under 35 USC §102(e) as being anticipated by Glass.

Independent claim 1 recites a method of personalizing an electronic signature device to a user. The electronic signature device includes a processor, a memory, a user input device including a first signature input device, and a device interface, all communicatively connected by at least one bus. According to the claimed method, a digitized written user signature of the user is received via the first signature input device. A prime parameter, a sub-prime parameter, and a base parameter are generated. A signing private key is generated. A signing public key is generated based on the prime, sub-prime, and base parameters. A user public key is generated based on the signing private key and the prime and base parameters. A biometric electronic template is generated based on the digitized written user signature. The prime, sub-prime, and base parameters, the signing private and public keys, and the biometric electronic template are stored in the memory.

In contrast, Glass discloses a method and apparatus for applying and verifying a biometric-based digital signature to an electronic document. According to the Glass method, an electronic document is "signed" using a hash value and a biometric value. First, a token value is added to the electronic document, and the hash function is applied

to the token-document combination to provide a hash value. See column 4, lines 27-39. A biometric reading is performed to provide a biometric value and a digital signature based on the biometric value, a secret key (which can be the private key of an asymmetric key pair). See column 4, lines 50-65. Later, an authentication process is performed.

Thus, Glass generates an electronic signature related to an electronic document, used by a recipient of the document to verify that the sender of the document is correctly identified, and that the document has not been tampered with during transmission. See column 6, lines 42-60. Glass does not disclose receiving a digitized written user signature, as recited in claim 1. The Glass signature is digital-only generated by the camera or other biometric value generator. The user signature recited in claim 1 is a written signature that has been digitized, and that is provided by the user via a signature input device.

Further, Glass does not disclose generation of prime, sub-prime, and base parameters on which a public key is based, as recited in claim 1. Also, Glass does not disclose generation of a biometric electronic template based on a digitized written user signature, as recited in claim 1. As noted above, Glass does not disclose any written signature at all, only an electronic signature generated by the biometric apparatus.

Thus, Glass discloses a method and apparatus that are fundamentally different than the claimed method. Glass discloses a system that electronically identifies a user with a document, generating an electronic "signature" based on the user's biometric input and other electronic values. The claimed invention, on the other hand, is a method of personalizing an electronic signature device to a user, utilizing the user's actual written

signature in digitized form to produce a biometric template stored in memory in the signature device, for future use by the user in, for example, binding the user's signature to a document.

For at least the reasons set forth above, it is submitted that Glass does not anticipate the invention recited in claim 1. Claims 2-25 depend from claim 1, and therefore also cannot be anticipated by Glass. The rejection of claims 1-25, therefore, should be withdrawn.

Independent claim 26 recites a method of originating an electronically signed transaction. An electronic signature device includes a processor, a memory having a biometric electronic template, a prime parameter, a sub-prime parameter, and a base parameter, user public data comprising a user public key, and a user private key stored therein, a user interface comprising a signature input device, a device interface adapted to interface a computer, and at least one bus operably connected to the processor, the memory, the user interface, and the device interface. According to the claimed method, verification takes place as to whether a user is permitted to originate the electronically signed transaction with the electronic signature device. This verification includes receiving a digitized written originator signature via the user interface, and comparing the digitized written originator signature against the biometric electronic template to produce a first verification result. A transaction package is received through either the user interface or the device interface. The transaction package and either the digitized originator signature or a digitized user signature extracted from the biometric electronic template are combined to produce an originator signature block. An ephemeral private

key is generated based on the prime, sub-prime, and base parameters. An ephemeral public key is generated based on the ephemeral private key and the prime and base parameters. A shared encryption key is generated based on the ephemeral public key, the user public key, and the prime parameter. The originator signature block is encrypted with the shared encryption key to produce an encrypted signature block. The encrypted signature block, the ephemeral private key, the prime parameter, and at least a portion of the user public data are combined to produce an electronically signed transaction. If the user is verified, the electronically signed transaction is provided via the device interface.

In contrast, Glass discloses a method and apparatus for applying and verifying a biometric-based digital signature to an electronic document. According to the Glass method, an electronic document is "signed" using a hash value and a biometric value. First, a token value is added to the electronic document, and the hash function is applied to the token-document combination to provide a hash value. See column 4, lines 27-39. A biometric reading is performed to provide a biometric value and a digital signature based on the biometric value, a secret key (which can be the private key of an asymmetric key pair). See column 4, lines 50-65. Later, an authentication process is performed.

Thus, Glass generates an electronic signature related to an electronic document, used by a recipient of the document to verify that the sender of the document is correctly identified, and that the document has not been tampered with during transmission. See column 6, lines 42-60. Glass does not disclose receiving a digitized written originator signature, as recited in claim 26. The Glass signature is digital-only generated by the camera or other biometric value generator. The originator signature recited in claim 26 is

a written signature that has been digitized, and that is provided by the originator via a signature input device.

Further, Glass does not disclose comparing the digitized written originator signature against a biometric electronic template, as recited in claim 26. As noted above, Glass does not disclose any written signature at all, only an electronic signature generated by the biometric apparatus. Also, Glass does not disclose generation of ephemeral private and public keys based on prime, sub-prime, and base parameters, as recited in claim 26.

Thus, Glass discloses a method and apparatus that are fundamentally different than the claimed method. Glass discloses a system that electronically identifies a user with a document, generating an electronic "signature" based on the user's biometric input and other electronic values. The claimed invention, on the other hand, is a method of originating an electronically signed transaction, utilizing the user's actual written signature in digitized form to verify permission to originate the transaction by comparing the signature against a biometric template stored in memory in the signature device.

For at least the reasons set forth above, it is submitted that Glass does not anticipate the invention recited in claim 26. Claims 27-38 depend from claim 26, and therefore also cannot be anticipated by Glass. The rejection of claims 26-38, therefore, should be withdrawn.

Based on the foregoing, it is submitted that all rejections have been overcome. It is therefore requested that the Amendment be entered, the claims allowed, and the case

passed to issue. If any issues remain outstanding, the examiner is encouraged to call the undersigned agent to attempt resolution in a telephone interview.

Respectfully submitted,

January 17, 2006
Date

Thomas M. Champagne
Registration No. 36,478
Customer Number 49691
(828) 253-8600

TMC:hlp